

TOOLBOX – INTERACTIVE CONTAINER ENVIRONMENT

ONDŘEJ MÍCHAL

Student, Intern at Red Hat

✉ harrymichal@fedoraproject.org

omichal@redhat.com

🌐 harrymichal.undo.it

harrymichal@freenode.net



Ondřej Míchal

- Information Technology Student at FIT BUT
- Intern at Desktop Team at Red Hat
 - *Since June 2019*
- Co-maintainer of Toolbox



Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

AGENDA

1) Introduction

a) Next-gen operating systems

b) Containers

c) Toolbox

2) Usage

3) Recent accomplishments & Plans for the future

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com





WHY TOOLBOX EXISTS?

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

IMAGE BASED OPERATING SYSTEMS



- Project Atomic, Fedora Silverblue, Fedora CoreOS, Fedora IoT
- NixOS, CoreOS, Flatcar
- Widely used term is also „immutable“. **Not accurate.**
- <https://blog.verbum.org> - Colin Walters
- Secure, reliable but clunky

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



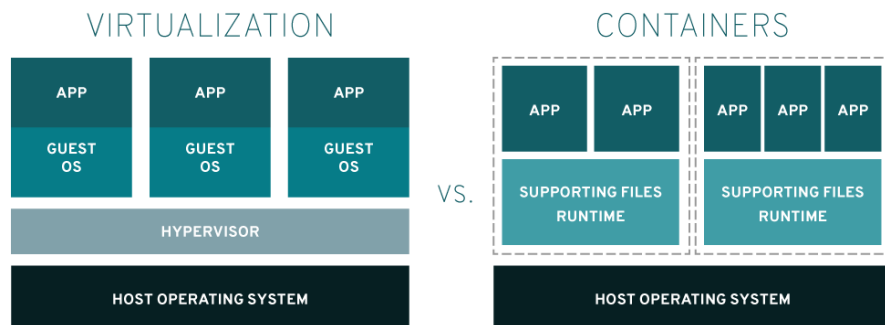
```
omichal@harry-work:~  
[omichal@harry-work ~]$ dnf  
bash: dnf: command not found  
[omichal@harry-work ~]$  
[omichal@harry-work ~]$ rpm-ostree status  
State: idle  
AutomaticUpdates: check; rpm-ostreed-automatic.timer: last run 8h ago  
Deployments:  
  ostree://fedora:fedora/rawhide/x86_64/silverblue  
    Version: Rawhide.20210216.n.1 (2021-02-16T18:48:26Z)  
    BaseCommit: 960fbb6ed2f96bca89ff36ffdd3bab5b94ff87331183cc9d8a8ff85f8cd152fa  
    GPGSignature: Valid signature by 787EA6AE1147EEE56C40B30CDB4639719867C58F  
    Diff: 53 upgraded, 1 removed, 1 added  
    LayeredPackages: ddcutil ffmpeg fish libva-intel-driver libva-utils neovim openssl tilix  
  ● ostree://fedora:fedora/rawhide/x86_64/silverblue  
    Version: Rawhide.20210214.n.0 (2021-02-14T06:03:46Z)  
    BaseCommit: ec454363b716324467fad59f6a718364c70e63fbbf5420cd9c2651f7cc69e95a  
    GPGSignature: Valid signature by 787EA6AE1147EEE56C40B30CDB4639719867C58F  
    LayeredPackages: ddcutil ffmpeg fish libva-intel-driver libva-utils neovim openssl tilix  
  ostree://fedora:fedora/rawhide/x86_64/silverblue  
    Version: Rawhide.20210208.n.0 (2021-02-08T06:07:03Z)  
    BaseCommit: 54615533ea9cde210a04139d6d4089928cdf5818790aled66b88f001afe05561  
    GPGSignature: Valid signature by 963A2BEB02009608FE67EA4249FD77499570FF31  
    LayeredPackages: ddcutil ffmpeg fish libva-intel-driver libva-utils neovim openssl tilix  
  ostree://fedora:fedora/rawhide/x86_64/silverblue  
    Version: Rawhide.20210113.n.0 (2021-01-13T06:11:33Z)  
    BaseCommit: 0d4f36faaab7dc4f3bd851084b95e1bec99f72bd522c28d80498ba992f19e176  
    GPGSignature: Valid signature by 963A2BEB02009608FE67EA4249FD77499570FF31  
    LayeredPackages: ffmpeg fish libva-intel-driver libva-utils neovim openssl tilix  
    Pinned: yes  
  ostree://fedora:fedora/32/x86_64/silverblue  
    Version: 32.20201107.0 (2020-11-07T02:00:39Z)  
    BaseCommit: 867d614a351cf3aacb0fccfbaea87084502fe3e5c45ed261b5e7e4036f433767  
    GPGSignature: Valid signature by 97A1AE57C3A2372CCA3A4ABA6C13026D12C944D0  
    LayeredPackages: dkms fish gcc libva libva-utils make neovim openssl tilix  
    LocalPackages: VirtualBox-6.1-6.1.16_140961_fedora32-1.x86_64  
    Pinned: yes  
AvailableUpdate:  
  Version: Rawhide.20210217.n.0 (2021-02-17T06:05:35Z)  
  Commit: 733af93a08c3d620d5248a063256602b65db0a1f0127b5f579a6ec022c63a9f9  
  GPGSignature: Valid signature by 787EA6AE1147EEE56C40B30CDB4639719867C58F  
  Diff: 71 upgraded, 2 removed, 3 added  
[omichal@harry-work ~]$
```

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

WILD CONTAINER SPOTTED

- Means to isolate applications with their entire runtime environment
- Containers share the kernel with the host system
- Much more lightweight than virtual machines



[\[1\] Virtualization vs. Container](#)

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



DOCKER!?



Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

DOCKER!?



Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



podman

daemonless container engine for developing, managing, and running OCI Containers on Linux systems

- Reimplementation of the Docker CLI
- Complements tools like Buildah and Skopeo
- Implemented with rootless containers in mind

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



“CLASSIC” USAGE OF CONTAINERS

- Easily disposable entities, rapid development – CI, CD
- Orchestration – Kubernetes
- Easy-to-run services – servers, databases,...

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



“CLASSIC” USAGE OF CONTAINERS

- Easily disposable entities, rapid development – CI, CD
- Orchestration – Kubernetes
- Easy-to-run services – servers, databases,...

DISPOSABLE & NON-INTERACTIVE

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



WHAT IS TOOLBOX?

Interactive container environment

- Built on top of Podman
- Brings the concept of toolboxes – pet containers
 - Persistent
 - Integrated

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



SOLUTION?



Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



SOLUTION?

Pet containers
=
Toolboxes

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



```
omichal@:/var/home/omichal
[omichal@harry-work ~]$ whereis dnf
dnf: /etc/dnf /usr/etc/dnf
[omichal@harry-work ~]$ toolbox enter -r 34
[omichal@toolbox omichal]$ whereis dnf
dnf: /usr/bin/dnf /etc/dnf
[omichal@toolbox omichal]$ ls -la /usr/bin/dnf
lrwxrwxrwx. 1 root root 5 Nov 23 17:43 /usr/bin/dnf -> dnf-3
[omichal@toolbox omichal]$
```

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

WHAT'S THE CATCH?

- Container setup cannot be changed
 - Mounts, entrypoint, network, seccomp, resource limits,...
- There is a lot to configure!

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



WHAT'S THE CATCH?

- Container setup cannot be changed
 - Mounts, entrypoint, network, seccomp, resource limits,...
- There is a lot to configure!

IS THERE A SOLUTION?

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



YES! AT LEAST PARTIALLY

- Mount as much as possible and cherry-pick
- Use a mechanism that allows dynamic change

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



YES! AT LEAST PARTIALLY

- Mount as much as possible and cherry-pick
- Use a mechanism that allows dynamic change

THE KEY IS THE
INITIAL CONFIGURATION
&
THE ENTRY-POINT

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



SMALL GLIMPSE UNDER THE HOOD



- Entry-point is Toolbox itself
- Mounts going under /run/host/
 - /boot, /etc, /dev, /run, /tmp, /var, /home, /usr
- Entry-point bind-mounts and symlinks, sets up user, sets up Kerberos, coredumpctl, journal,...

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

SMALL GLIMPSE UNDER THE HOOD



- Entry-point is Toolbox itself
- Mounts going under /run/host/
 - /boot, /etc, /dev, /run, /tmp, /var, /home, /usr
- Entry-point bind-mounts and symlinks, sets up user, sets up Kerberos, coredumpctl, journal,...

PERSISTENCE & INTERACTIVITY

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

SMALL GLIMPSE UNDER THE HOOD



```
"HostConfig": {
  "Binds": [
    "/var:/run/host/var:slave,rw,rbind",
    "/run:/run/host/run:slave,rw,nosuid,nodev,rbind",
    "/run/media:/run/media:slave,rw,nosuid,nodev,rbind",
    "/etc:/run/host/etc:rw,rprivate,rbind",
    "/run/dbus/system_bus_socket:/run/dbus/system_bus_socket:rw,rprivate,nosuid,nodev,rbind",
    "/usr/bin/toolbox:/usr/bin/toolbox:ro,rprivate,rbind",
    "/etc/profile.d/toolbox.sh:/etc/profile.d/toolbox.sh:ro,rprivate,rbind",
    "/run/user/1000:/run/user/1000:rw,rprivate,nosuid,nodev,rbind",
    "/boot:/run/host/boot:slave,rw,rbind",
    "/usr:/run/host/usr:ro,slave,rbind",
    "devpts:/dev/pts",
    "/run/.heim_org.h5l.kcm-socket:/run/.heim_org.h5l.kcm-socket:rw,rprivate,nosuid,nodev,rbind",
    "/var/home/omichal:/var/home/omichal:slave,rw,rbind",
    "/dev:/dev:slave,rw,noexec,nosuid,rbind",
    "/tmp:/run/host/tmp:slave,rw,nosuid,nodev,rbind"
  ],
```

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

SMALL GLIMPSE UNDER THE HOOD



```
"Id": "cd32f1662c2b0aedcc4e979ca2f32aba88643a2fc881cf5967d0d91c6c5ba655",  
"Created": "2020-12-08T01:08:45.291446036+01:00",  
"Path": "toolbox",  
"Args": [  
  "--verbose",  
  "init-container",  
  "--home",  
  "/home/omichal",  
  "--home-link",  
  "--media-link",  
  "--mnt-link",  
  "--monitor-host",  
  "--shell",  
  "/bin/fish",  
  "--uid",  
  "1000",  
  "--user",  
  "omichal"  
],
```

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

TALK TOPICS

1) *Introduction*

2) Usage

a) On Fedora Silverblue

b) On RHEL 8

3) Recent accomplishments & Plans for the future

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



DEMO



TALK TOPICS

1) *Introduction*

2) *Usage*

3) **Recent accomplishments & Plans for the future**

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



ACCOMPLISHMENTS

- Toolbox will be shipped in RHEL 8.4
- Allowed the rootfull use-case
- Added support for RHEL (resp. UBI)
 - Foundation for adding support for other distros
- Added Toolbox-specific tests to Podman
- A lot of polish and bugfixes

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



FUTURE PLANS

- Better customization
- More intuitive CLI UI
- Robust means to invoke commands on the host
- More tests!

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com



QUESTIONS?



GET IN TOUCH!

<https://github.com/containers/toolbox>

Reports, patches and productive discussion are very welcome!



Debarshi Ray
maintainer



Ondřej Míchal
maintainer

Ondřej Míchal

✉ harrymichal@fedorapeople.org; omichal@redhat.com

